Cisco E メール セキュリティ アプライアンス

企業では毎日 1,000 億以上の E メール メッセージがやり取りされています。E メールの使用が増えるにつれ、セキュリティの優先度はさらに高くなっていきます。シスコ® のソリューションは、組織にとって大きなセキュリティ課題となっている、ダイナミックで急激に変化する脅威に対し、可用性の高い E メール保護を実現します。

機能と利点

シスコの E メール セキュリティ ソリューションは、物理、仮想、クラウド、ハイブリッドのいずれの分野においても業界をリードするソリューションとして、以下のメリットを実現します。

- **迅速で包括的な保護**:他社製品よりも数時間または数日早い対応が可能。
- **最大規模の脅威インテリジェンス ネットワーク**:Cisco Talos による広範で総合的なセキュリティ分析を活用。
- **アウトバウンド メッセージの保護**:オンデバイスのデータ損失防止(DLP)、E メール暗号化、さらに RSA エンタープライズ DLP ソリューションとの統合(オプション)によってメッセージを保護。
- **総所有コストの低減**:省スペース、簡単実装、自動管理によりコストを長期的に削減。

製品概要

迷惑メールやマルウェアは、インバウンドの脅威やアウトバウンドのリスクなどの、E メール セキュリティをめぐる複雑な状況の一部にすぎなくなりました。オールインワンの Cisco E メール セキュリティ アプライアンスは、シンプルで迅速な導入、省メンテナンス、低遅延、運用コストの削減をもたらします。シスコの「Set and forget」テクノロジーでは、初期の自動ポリシー設定が実行されれば、あとは管理者の手を煩わせることがありません。その後、セキュリティのアップデートをシスコのクラウドベースの脅威インテリジェンス ソリューションに自動的に転送します。この E メール アプライアンスでは、脅威インテリジェンス データが 3 ～ 5 分ごとに更新されます。これにより、他のベンダーよりも数時間または数日早く最新の防御対策を講じることができます。柔軟な導入オプションと、既存のインフラストラクチャとのスムーズな統合を実現するこのアプライアンスは、ビジネス ニーズに最適なソリューションです。

仮想アプライアンス

Cisco E メール セキュリティ仮想アプライアンスは、特に大規模な分散ネットワーク環境における Web セキュリティ導入コストの大幅削減に貢献します。このアプライアンスを利用すると、ネットワーク マネージャは既存のネットワーク インフラストラクチャを使って、必要なときに、必要な場所にインスタンスを作成できます。この物理アプライアンスのソフトウェア バージョンは、VMware ESXi Hypervisor と Cisco Unified Computing System™（Cisco UCS®）サーバ上で動作します。Cisco E メール セキュリティ ソフトウェア バンドルを購入すると、この仮想アプライアンスの無制限ライセンスが提供されます。

この仮想アプライアンスを使用することにより、シンプルなキャパシティ プランニングでトラフィックの増大にすばやく対応できます。アプライアンスの購入や発送は必要ないため、データセンターを複雑化したり、人員を追加したりしなくても、新たなビジネス チャンスをサポートできます。

主要な機能

ミッション クリティカルな E メール システムを、物理、仮想、クラウド、ハイブリッドのソリューションで保護します。表 1 に、シスコの E メール セキュリティ ソリューションの主要な機能の概要を示します。

偽装メールの検出は、上級幹部（高価値標的とも呼ばれる）を狙うスピーフィング攻撃から保護します。この機能は、専用コンテンツ フィルタによってこれらのカスタマイズされた攻撃をブロックします。また、すべての試行および実施されたアクションに対する詳細なログを取得します。

表 1. 主要な機能

機能	説明
グローバル脅威インテリジェンス	世界最大級の脅威検知ネットワークをベースとした、迅速かつ包括的な E メール保護を受けられます。シスコは以下のような広範な可視性と最大級の規模を実現しています。 • 毎日 100 TB のセキュリティ インテリジェンス • ファイアウォール、Cisco IPS センサー、Web および E メール アプライアンスなどの、160 万台のセキュリティ デバイス • 1 億 5,000 万台のエンドポイント • 1 日あたり 130 億件の Web 要求 • 世界のエンタープライズ E メール トラフィックの 35 % Cisco Talos は、グローバルなトラフィック アクティビティを 24 時間体制で表示し、問題点の分析、新しい脅威の検出、トラフィック トレンドのモニタを行います。Talos は、ルールを継続的に生成し、そのアップデートをセキュリティ アプライアンスへ適用することで、ゼロアワー攻撃を防止します。こうしたアップデートは 3 ～ 5 分おきに実行され、業界トップクラスの脅威防御を実現します。
迷惑メールのブロック	迷惑メールは複雑な問題で、高度なソリューションが必要です。シスコなら簡単に対応できます。迷惑メールがお客様の受信ボックスに到達するのを止めるため、送信者のレピュテーションに基づいてフィルタリングを行う外層と、メッセージを詳細に分析するフィルタリングの内層を組み合わせた多層防御策を講じています。レピュテーション フィルタリングでは、80 % 以上の迷惑メールがネットワークへ侵入する前にブロックされます。最新の機能強化によって、コンテキストの分析、高度な自動化、および自動分類が導入され、Snowshoe 攻撃に対する強力な対策が可能になっています。 短時間で大量の E メールを受信するお客様は、送信者や件名に基づくフィルタを適用できます。このフィルタでは、条件に関連するメッセージがブロックまたは隔離されます。
グレーメールの検出と安全な配信停止	グレーメールには、マーケティング、ソーシャル ネットワーキング、バルク メッセージなどが含まれます。このグレーメール検出機能は、組織が受信するグレーメールに対する正確な分類と監視に役立ち、管理者は、カテゴリに応じて適切なアクションを取ることができます。多くの場合、グレーメールには配信停止リンクが含まれています。このリンクを使用して、エンド ユーザは当該メールの配信停止を希望することを送信者に通知します。このような配信停止メカニズムの偽装はフィッシングの手口であることが多いため、ユーザはこうした配信停止リンクをクリックする際は注意しなければなりません。 この安全な配信停止ソリューションは、以下を実現します。 • 配信停止リンクを装った悪意のある脅威に対する防御 • すべての登録を管理するための統一されたインターフェイス • 配信停止リンクを含んだ E メールに対する E メール管理者およびエンドユーザの可視性の向上
高度なマルウェア防御（AMP）	Cisco E メール セキュリティ アプライアンスには、Cisco Advanced Malware Protection が含まれています。このアプライアンスは、ファイル レピュテーション スコアおよびブロック、静的、動的両方のファイル分析機能（サンドボックス）、ファイル レトロスペクション機能を備え、脅威が E メール ゲートウェイを通過した後も、継続的に分析を行います。ユーザはこれまで以上に多くの攻撃をブロックし、不審なファイルを追跡できるほか、アウトブレイク範囲の軽減および迅速な修復が可能です。高度なマルウェア防御は追加のライセンス機能として、すべての E メール セキュリティ アプライアンスをお使いのお客様にご利用いただけます。Cisco AMP Threat Grid は、マルウェア サンプルのクラウドへの送信に対してコンプライアンスまたはポリシー制限を設けている組織向けに、オンプレミスのアプライアンスを使用してマルウェア防御を実現します。 AMP システムを、AMP プライベート クラウド ライセンスを使用して完全にオンプレミスに導入できるようになりました。これは AMP パブリック クラウドを使用できない厳格なポリシー要件がある顧客にとって重要で、AMP パブリック クラウドの更新を引き続き活用できます。 AMP レトロスペクティブ セキュリティの Office 365 ユーザ向けのマルウェア自動修復機能により、短時間で手間をかけずに侵害を修復できます。ユーザ側の操作は、このような感染したメールに対して自動的にアクションを実行するようメール セキュリティ ソリューションを設定することだけです。

機能	説明
アウトブレイク フィルタ	アウトブレイク フィルタは、新しい脅威や複合型の攻撃に対処します。このフィルタでは、ファイルの種類、ファイル名、ファイル サイズ、メッセージ内の URL など 6 種類のパラメータを任意に組み合わせてルールを発行することができます。Talos がアウトブレイクの詳細を把握すると、ルールを変更し、それに応じて検疫領域からメッセージを送信します。アウトブレイク フィルタは、疑わしいメッセージ内の URL を書き換えることもできます。この新しい URL をクリックすると、受信者は Cisco Web セキュリティ プロキシを介してリダイレクトされます。当該の Web サイトのコンテンツはアクティブにスキャンされ、サイトにマルウェアが含まれている場合はアウトブレイク フィルタがブロック画面を表示します。
Web インタラクション トラッキング	この完全に統合されたソリューションにより、IT 管理者は、E メール セキュリティ アプライアンスで書き換え済みの URL をクリックしたエンドユーザを追跡することができます。レポートには以下の内容が表示されます。 • 悪意のある URL のクリック回数が上位のユーザ • エンドユーザによるクリック回数が上位の悪意のある URL • 日時、書き換えの理由、その URL に対して実行されたアクション 管理者は、特定の URL が含まれたすべてのメッセージをトレース バックすることもできます。
アウトバウンド メッセージの制御	E メール セキュリティ アプライアンスはアウトバウンド メッセージを DLP E メール暗号化によって制御します。この制御により、最も重要なメッセージが確実に業界標準に準拠し、転送中に保護されます。さらに、アウトバウンド レート制限とともにアウトバウンド アンチスパムやアンチウイルス スキャンを利用すれば、侵害されたマシンやアカウントにより、組織が E メールのブラックリストに入れられるのを防ぐことができます。また、新機能として、E メール セキュリティ アプライアンスは Transport Layer Security（TLS）に加えて、Secure/Multipurpose Internet Mail Extensions（S/MIME）暗号化および署名をサポートします。
偽装メールの検出	偽装メールの検出は、幹部（高価値標的とも呼ばれる）を狙うスピーフィング攻撃から保護します。この機能は、専用コンテンツ フィルタによってこれらのカスタマイズされた攻撃をブロックします。また、すべての試行および実施されたアクションに対する詳細なログを取得します。
優れたパフォーマンス	このセキュリティ アプライアンスは、新規のインバウンド E メール ウイルスをすばやくブロックします。ドメイン配信キューでは、その他ドメイン向けの重要な配信物のバックアップとして、不達の E メールを保持します。このソリューションは、99.9 % を超える業界トップクラスの迷惑メール捕捉率と、100 万分の 1 未満の誤検知を実現します。
DLP	定義済みのポリシーを 1 つ以上使用して（選択できるポリシーは 100 以上）、機密データがネットワーク外に流出するのを防止できます。定義済みポリシーの一部をカスタマイズして独自のポリシーを作成することもできます。標準搭載の RSA E メール DLP エンジンは、文字、フレーズ、辞書、正規表現などのオプションのデータ ポイントと併せて調整済みのデータ構造を使用し、誤検出がほとんど発生しない正確なポリシーをすばやく作成します。DLP エンジンでは、深刻度に応じて違反をスコア判定します。これにより、ニーズに合わせて異なるレベルの修復を適用することができます。
低コスト	省スペースで簡単なセットアップ、自動化されたアップデート管理を実現する E メール セキュリティ ソリューションは、コスト削減にも効果があります。シスコのソリューションは、市場で最高レベルの TCO を実現します。
柔軟な導入	すべての Cisco E メール セキュリティ ソリューションは、同じ方法で簡単に導入できます。システム セットアップ ウィザードは、複雑な環境にも対応します。わずか数分でシステムを開始、保護し、より安全な環境へとすばやく移行できます。ライセンスは、デバイス ベースではなくユーザ ベースです。デバイス単位ではなくユーザ単位で、インバウンドのみならずアウトバウンドの E メール ゲートウェイ保護を追加料金なしで適用できます。これにより、スパム対策エンジンやウイルス対策エンジンでアウトバウンド メッセージをスキャンでき、ビジネス ニーズを完全にサポートできます。 仮想アプライアンスは物理アプライアンスの機能をすべて備えながら、仮想導入モデルの利便性とコスト節約のメリットも得られます。また、インスタント セルフサービス プロビジョニングも含まれています。Cisco E メール セキュリティ仮想アプライアンス ライセンスを使用すれば、E メール セキュリティ ゲートウェイをインターネット接続なしでご使用のネットワークに導入できます。このライセンスには、ソフトウェア ライセンスが付属しています。新たにローカルへ保存した仮想イメージ ファイルには、いつでもライセンスを適用できます。元の仮想イメージ ファイルは、複数の E メール セキュリティ ゲートウェイをすばやく導入するために、必要に応じてクローン作成できます。 ハードウェアと仮想 E メール セキュリティ ソリューションを同じ環境で実行できます。そのため、小規模なブランチ オフィスや離れた場所にも、本社と同等の保護を適用できます。各拠点にハードウェアを設置し、サポートする必要はありません。Cisco コンテンツ セキュリティ管理アプライアンス、または Cisco コンテンツ セキュリティ管理仮想アプライアンスを使用すると、カスタム導入環境を簡単に管理できます。
ビジネスにフィットするソリューション	Cisco クラウド E メール セキュリティは、ソフトウェア、コンピューティング能力、サポートを備えた、信頼性の高い包括的なサービスです。共通管理されるユーザ インターフェイスは、シスコの物理および仮想 E メール セキュリティ アプライアンスのユーザ インターフェイスと同じです。そのため、管理負担を最小限に抑えることができ、モニタおよび管理するためのハードウェアをオンサイトに設置せずに優れた保護を実施できます。Microsoft Office 365 の顧客は、Office 365 向けのクラウド E メール セキュリティと同等の業界最先端の保護機能も利用できます。このソリューションは導入が簡単で、高レベルのサービス可用性とデータ保護を備えた複数の復元力あるデータセンターを通じて確実な信頼性が保証されます。 ハイブリッド ソリューションでは、オンサイトで重要なメッセージに対して高度なアウトバウンド制御を実行しながら、クラウドのコスト効果や利便性を活用できます。 契約期間を通じて、ユーザの総数が同じであれば、オンプレミスとクラウドのユーザ数を変更できます。このように、組織のニーズが変化しても柔軟に対応できます。 オンプレミスのハードウェアおよび仮想アプライアンスはすぐに設置できるようになっており、自社の環境に最適なモデルを選択して、インバウンドとアウトバウンドのメッセージをゲートウェイで保護することができます。

製品仕様

表 2 に E メール セキュリティ アプライアンスのパフォーマンス仕様を、表 3 にアプライアンスのハードウェア仕様、表 4 に仮想アプライアンスの仕様、そして表 5 にセキュリティ管理アプライアンスの仕様をそれぞれ示します。

表 2. E メール セキュリティ アプライアンスのパフォーマンス仕様

導入対象	モデル	ディスク領域	RAID のミラーリング	メモリ	CPU
大規模企業	ESA C690	2.4 TB（600 GB X 4）	対応（RAID 10）	32 GB DDR4	2 X 2.4 GHz、6 コア
大規模企業	ESA C690X	4.8 TB（600 GB X 8）	対応（RAID 10）	32 GB DDR4	2 X 2.4 GHz、6 コア
大規模企業	ESA C680	1.8 TB（300 GB X 6）	対応（RAID 10）	32 GB DDR3	2 X 2.0 GHz、6 コア
中規模企業	ESA C390	1.2 TB（600 GB X 2）	対応（RAID 1）	16 GB DDR4	1 X 2.4 GHz、6 コア
中規模企業	ESA C380	1.2 TB（600 GB X 2）	対応（RAID 1）	16 GB DDR3	1 X 2.0 GHz、6 コア
中小規模の企業またはブランチ オフィス	ESA C190	1.2 TB（600 GB X 2）	対応（RAID 1）	8 GB DDR4	1 X 1.9 GHz、6 コア
中小規模の企業またはブランチ オフィス	ESA C170	500 GB（250 GB X 2）	対応（RAID 1）	4 GB DDR3	1 X 2.8 GHz、デュアル コア

注：正確なサイジングが必要な場合は、シスコのコンテンツ セキュリティ スペシャリストとともにピーク メールフロー レートと平均メッセージ サイズを確認してください。

表 3. E メール セキュリティ アプライアンスのハードウェア仕様

モデル	ESA C690	ESA C690X	ESA C680	ESA C390	ESA C380	ESA C190	ESA C170
ラック ユニット（RU）	2 RU	2 RU	2 RU	1 RU	2 RU	1 RU	1 RU
寸法（高さ X 幅 X 奥行）	8.6 X 48.3 X 73.7 cm（3.4 X 19 X 29 インチ）	8.6 X 48.3 X 73.7 cm（3.4 X 19 X 29 インチ）	8.9 X 48.3 X 73.7 cm（3.5 X 19 X 29 インチ）	4.3 X 48.3 X 78.7 cm（1.7 X 19 X 31 インチ）	8.9 X 48.3 X 73.7 cm（3.5 X 19 X 29 インチ）	4.3 X 48.3 X 78.7 cm（1.7 X 19 X 31 インチ）	4.24 X 42.9 X 39.4 cm（1.67 X 16.9 X 15.5 インチ）
DC 電源オプション	対応	対応	対応	非対応	対応	非対応	非対応
リモートによる電源の再投入	対応	対応	対応	対応	対応	非対応	非対応
冗長電源	対応	対応	対応	対応	対応	対応（アクセサリ オプション）	非対応
ホットスワップ可能ハード ディスク	対応	対応	対応	対応	対応	対応	対応
イーサネット インターフェイス	6 ポート 1GBASE-T 銅線ネットワーク インターフェイス（NIC）、RJ-45	6 ポート 1GBASE-T 銅線ネットワーク インターフェイス（NIC）、RJ-45	6 ポート 1GBASE-T 銅線ネットワーク インターフェイス（NIC）、RJ-45	6 ポート 1GBASE-T 銅線ネットワーク インターフェイス（NIC）、RJ-45	6 ポート 1GBASE-T 銅線ネットワーク インターフェイス（NIC）、RJ-45	2 ポート 1GBASE-T 銅線ネットワーク インターフェイス（NIC）、RJ-45	2 ポート 1GBASE-T 銅線ネットワーク インターフェイス（NIC）、RJ-45
速度（Mbps）	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション	10/100/1000、オートネゴシエーション

モデル	ESA C690	ESA C690X	ESA C680	ESA C390	ESA C380	ESA C190	ESA C170
ファイバ オプション	あり（別個の SKU） 6 ポート 1GBASE-SX 光ファイバ：ESA-C690-1G 6 ポート 10GBASE-SR 光ファイバ：ESA-C690-10G	あり（別個の SKU） 6 ポート 1GBASE-SX 光ファイバ：ESA-C690-1G 6 ポート 10GBASE-SR 光ファイバ：ESA-C690-10G	あり（別個の SKU） 6 ポート 1GBASE-SX 光ファイバ：ESA-C690-1G 6 ポート 10GBASE-SR 光ファイバ：ESA-C690-10G	なし	なし	なし	なし

表 4. E メール セキュリティ仮想アプライアンスの仕様

E メール ユーザ				
	モデル	**ディスク**	**メモリ**	**コア**
評価のみ	ESAV C000v	200 GB（10K RPM SAS）	4 GB	1（2.7 GHz）
小規模企業（従業員 1,000 人まで）	ESAV C100v	200 GB（10K RPM SAS）	6 GB	2（2.7 GHz）
中規模企業（従業員 5,000 人まで）	ESAV C300v	500 GB（10K RPM SAS）	8 GB	4（2.7 GHz）
大規模企業またはサービス プロバイダー	ESAV C600v	500 GB（10K RPM SAS）	8 GB	8（2.7 GHz）
サーバ				
Cisco UCS	VMware ESXi 5.0、5.1、5.5 ハイパーバイザ			

表 5. セキュア管理アプライアンス M シリーズ プラットフォームの仕様

モデル	SMA M690/690X/680	SMA M390/380	SMA M190/M170
ユーザ数	10,000 人以上	10,000 人以下	1,000 人以下

導入先

E メール セキュリティ ソリューションは以下に導入できます。

- **オンプレミス**：E メール セキュリティ アプライアンスはゲートウェイとして、通常、ファイアウォール外部のネットワーク エッジ（通称「緩衝地帯」）に導入します。受信した Simple Mail Transfer Protocol（SMTP）トラフィックは、メール交換レコードで設定した仕様に従って、このアプライアンスのデータ インターフェイスに転送されます。アプライアンスはそのメールをフィルタリングし、ネットワークのメール サーバに再転送します。一方のメール サーバも発信メールをデータ インターフェイスに送ります。メールはそこで発信ポリシーに従ってフィルタリングされ、外部の宛先に送信されます。
- **仮想**：小規模なブランチ オフィスで Cisco UCS が実行されている場合、この仮想アプライアンスを Cisco Web セキュリティ仮想アプライアンスなどの他のシスコ製品でホストすることができます。同等のハードウェアと同レベルの保護が提供されますが、スペースや電力を節約できます。このカスタム導入は、セキュリティ管理アプライアンスまたはセキュリティ管理仮想アプライアンスで一元管理できます。

クラウド セキュリティのオプション

Cisco クラウド E メール セキュリティは、柔軟な E メール セキュリティの導入モデルを提供します。共通管理できるほか、オンサイトで E メール セキュリティ インフラストラクチャを管理する必要がないので、コストを削減できます。

Cisco ハイブリッド E メール セキュリティは、クラウド E メール セキュリティのメリットを実現しながら、メッセージの暗号化とオンサイト DLP による高度なアウトバウンド制御を行います。ハイブリッド ソリューションであれば、自分のペースでクラウド ソリューションへの移行を進められます。

Cisco E メール セキュリティ：物理アプライアンスと仮想アプライアンスのライセンス

仮想アプライアンスのライセンスは、すべての E メール セキュリティ ソフトウェア バンドル（Cisco E メール セキュリティ インバウンド、E メール セキュリティ アウトバウンド、および E メール セキュリティ プレミアム）に含まれています。このライセンスの期間は、バンドル内のその他ソフトウェア サービスと同様で、購入したユーザ数を超えなければ、必要な数の仮想マシンで使用できます。この E メール セキュリティ アプライアンスのライセンスは、すべての E メール セキュリティ ソフトウェア バンドルに含まれています。あとは、サポートが必要なメールボックス数に適したライセンスを購入し、適切なオンプレミス アプライアンスを購入するだけです。仮想アプライアンスについては、ソフトウェア ライセンスを注文して権限付与を受けてください。

期間ベースのサブスクリプション ライセンス

ライセンスは、期間ベースのサブスクリプション（1 年、3 年、5 年）です。

数量ベースのサブスクリプション ライセンス

Cisco E メール セキュリティのポートフォリオでは、メールボックス数に基づき段階的価格を設定しています。お客様に適した導入の決定は、販売代理店およびパートナーの代理店がお手伝いします。

E メール セキュリティのソフトウェア ライセンス

E メール セキュリティ ソフトウェア ライセンス バンドルには、Cisco E メール セキュリティ インバウンド、Cisco E メール セキュリティ アウトバウンド、Cisco E メール セキュリティ プレミアムの 3 種類があります。高度なマルウェア防御は別途購入できます。各ソフトウェア製品の主要なコンポーネントを表 6 に示します。

表 6. ソフトウェア コンポーネント

バンドル	説明
Cisco E メール セキュリティ インバウンド Essentials	Cisco E メール セキュリティ インバウンド Essentials バンドルは、E メールベースの脅威から保護します。これにはグレーメール検出機能を備えたスパム対策、Sophos Antivirus ソリューション、ウイルス アウトブレイク フィルタ、偽装メールの検出、およびクラスタリングが含まれます。
Cisco E メール セキュリティ アウトバウンド Essentials	Cisco E メール セキュリティ アウトバウンド Essentials バンドルは、データ損失の防止（DLP）コンプライアンス、E メール暗号化、およびクラスタリングを提供します。
Cisco E メール セキュリティ プレミアム	Cisco E メール セキュリティ プレミアム バンドルは、上記の 2 つの Cisco E メール セキュリティ Essentials ライセンスに含まれるインバウンドとアウトバウンドの保護を組み合わせたもので、E メールベースの脅威からの保護と基本的なデータ損失の防止を提供します。
スタンドアロン製品	**説明**
Cisco Advanced Malware Protection	Cisco Advanced Malware Protection は、他の Cisco E メール セキュリティ ソフトウェア バンドルと併せてご購入いただけます。AMP は包括的なマルウェア回避ソリューションで、マルウェアの検出とブロック、継続的な分析、および遡及的なアラートが可能です。 Advanced Malware Protection は、すでに Cisco E メール セキュリティ アプライアンスで提供されているアンチマルウェアの検出およびブロック機能を強化します。ファイル レピュテーション スコアおよびブロック、静的、動的両方のファイル分析機能（サンドボックス）、およびファイル レトロスペクション機能を備え、脅威が E メール ゲートウェイを通過した後も継続的に分析を行います。必要なハードウェアを購入すると、AMP Threat Grid の無制限ライセンスが付与されます。そして AMP システムは、Threat Grid アプライアンスとともに、AMP プライベート クラウド ライセンスを使用して完全にオンプレミスに導入できるようになりました。これは AMP パブリック クラウドを使用できない厳格なポリシー要件がある顧客にとって重要です。
グレーメールの安全な配信停止	グレーメールに安全な配信停止オプションをタグ付けできるようになりました。このタグは、エンドユーザに代わって「配信停止」アクションを安全に管理します。また、各種のグレーメール配信停止要求をモニタします。これらはすべて、LDAP グループ ポリシー レベルで管理できます。

ソフトウェア ライセンス契約

ソフトウェア ライセンスを購入すると、それぞれについてシスコ エンドユーザ ライセンス契約および Web セキュリティの補足エンド ユーザ ライセンス契約が提供されます。

ソフトウェア サブスクリプションのサポート

すべての E メール セキュリティのライセンスには、ビジネスに不可欠なアプリケーションを利用可能にして、安全かつ最高のパフォーマンスで運用するために必要なソフトウェア サブスクリプション サポートが含まれています。このサポートによって、お客様は購入したソフトウェア サブスクリプションの全期間にわたって、以下に示すサービスを利用できます。

- ソフトウェア更新およびメジャー アップグレードを適用し、最新機能で最適なアプリケーションのパフォーマンスを得る
- Cisco Technical Assistance Center から専門的なサポートをすばやく受ける
- 社内の専門知識を構築して拡張し、ビジネスの俊敏性を高めるオンライン ツールを利用する
- 追加的な知識習得とトレーニングの機会を提供するコラボレーション性の高い学習

シスコ サービス

表 7 に、E メール セキュリティ ソリューションで利用できるシスコ サービスの概要を示します。

表 7. シスコ サービス

サービス	説明
シスコ ブランド サービス	• シスコのセキュリティの計画と設計サービスでは、堅牢なセキュリティ ソリューションを迅速かつコスト効率よく導入できます。 • Cisco E メール セキュリティ設定およびインストール リモート サービスでは、ソリューションのインストール、設定、テストを通じてセキュリティ リスクの軽減を図ります。 • Cisco Security Optimization Service は、新たなセキュリティの脅威、設計、パフォーマンスのチューニング、システム変更のサポートなど、進化するセキュリティ システムをサポートします。
コラボレーション/パートナー サービス	• シスコ コラボレーション プロフェッショナル サービスのネットワーク デバイス セキュリティ アセスメント サービスは、セキュリティのギャップを特定することで堅牢なネットワーク環境を維持します。 • Cisco Smart Care Service は、ネットワークのパフォーマンスを安全に可視化し、そこで得られた情報を基に予防的なモニタリングを実施して、ビジネスを最良の状態で運営できるようにします。 • このほか、シスコ パートナーが計画、設計、導入、最適化のライフサイクルを通じて、幅広い有益なサービスを提供します。
シスコのファイナンス	Cisco Capital® は、ビジネス ニーズに合わせて融資ソリューションをカスタマイズします。シスコのテクノロジーを早めに取り入れれば、それだけ早くビジネス メリットを得ることができます。

Cisco Smart Net Total Care サポート サービス

テクノロジーへの投資価値を最大化するために、E メール セキュリティ アプライアンスと併せて Cisco Smart Net Total Care™ サービスを購入することをお勧めします。このサービスを利用することにより、シスコの専門家やセルフサービスのサポート ツールにいつでも直接アクセスしてネットワークの問題をすばやく解決できるほか、ハードウェアを迅速に交換することもできます。詳細については、http://www.cisco.com/c/en/us/services/support/smart-net-total-care.html [英語] を参照してください。

Cisco E メール セキュリティ アプライアンスの評価方法

Cisco E メール セキュリティ アプライアンス C シリーズまたは X シリーズ プラットフォームの利点を理解する最良の方法は、Try Before You Buy 評価プログラムに参加していただくことです。ネットワーク内のテストを行うための全機能を備えた評価用アプライアンス（45 日間無料）をご希望の場合は、こちらのページ [英語] にアクセスしてください。

Cisco クラウド E メール セキュリティ サービスの評価方法

クラウド ベース ソリューションは、E メール セキュリティに対して柔軟な導入モデルを提供する、信頼性が高く、すべてを包含したサービスです。共通管理できるほか、オンサイトで E メール セキュリティ インフラストラクチャを管理する必要がないので、コストを削減できます。45 日間の無料評価の設定については、シスコ アカウント チームまたは販売代理店にお問い合わせください。

Cisco E メール セキュリティ仮想アプライアンスの評価方法

1. http://www.cisco.com/jp/go/esa/ にアクセスします。
2. 右側の [サポート（Support）] の下の、[ソフトウェアのダウンロード、リリース情報および一般情報（Software Downloads, Release and General Information）] をクリックします。[ソフトウェアのダウンロード（Download Software）] をクリックしたら、いずれかのモデルをクリックして、ダウンロード可能な仮想マシンのイメージを探します。このほか、ダウンロード可能な XML 評価ライセンスもあります。いずれかのイメージと XML 評価ライセンスをダウンロードする必要があります。
3. Cisco.com から、次のドキュメントをダウンロードします。
   a. シスコ セキュリティ仮想アプライアンス インストール ガイド [英語]
   b. Cisco AsyncOS® 9.5 for Email リリース ノート [英語]
4. Cisco セキュリティ仮想アプライアンスのインストール ガイドの指示に従い、インストールを開始します。Cisco コンテンツ セキュリティ仮想アプライアンスの評価は Cisco Smart Net Total Care サービスのサポート対象外です。ご注意ください。

保証に関する情報

保証については、Cisco.com の製品保証 [英語] のページを参照してください。

シスコが選ばれる理由

セキュリティは、組織のネットワークにとってかつてないほど重要になっています。機密保持や制御に関する懸念に加え、脅威やリスクが存在する限り、ビジネスの継続性を提供し、貴重な情報を保護し、ブランドへの評価を維持するために、セキュリティは不可欠です。シスコの統合セキュリティ ソリューションをネットワーク ファブリックに組み込むことで、優れた可視性と制御性を実現し、ビジネスを中断させることなく、お客様のビジネスを保護できます。セキュリティ市場のリーダーとして、攻撃前、攻撃中、攻撃後の各フェーズにわたる高度な脅威への対策を実現し、革新的な製品群と豊かな経験を持つシスコは、お客様のセキュリティ ニーズを満たす最適なベンダーであると言えます。

Cisco Capital

目標の達成を支援するファイナンス

Cisco Capital ファイナンス プログラムは、目的達成と競争力の維持に必要なテクノロジーの調達をサポートします。お客様の CapEx を削減し、成功を加速させ、投資金額と ROI を最適化します。Cisco Capital ファイナンス プログラムにより、ハードウェア、ソフトウェア、サービス、および補完的なサードパーティ製機器を柔軟に購入することができます。また、それらの購入を 1 つにまとめた計画的なお支払い方法をご用意しています。Cisco Capital は 100 ヵ国以上でサービスを利用できます。詳細はこちら

関連情報

詳細については、http://www.cisco.com/go/emailsecurity [英語] を参照してください。または、弊社の E メール セキュリティを無料で試用する 3 つの方法 [英語] を参照してください。

お問い合せ先

シスコシステムズ合同会社
〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

C78-729751-11JA 16.08